REMARKS/ARGUMENTS

This Amendment is in response to the Final Office Action dated January 23, 2006. Claims 1-14 are pending. Claims 1-14 are rejected. Claim 7 has been amended. Accordingly, claims 1-14 remain pending in the present application.

This amendment is seen by Applicant as broadening or cosmetic, and as such, is not subject to the prosecution history estoppel imposed by Festo. For the record, Applicant points out that the Supreme Court in Festo noted that a cosmetic amendment would not narrow the patent's scope and thus would not raise the estoppel bar.

This response is submitted in accordance with Rule 116 in an earnest effort to put the application in better condition for allowance. It is believed that Applicant's response has not amended the claims in a way that would raise new issues for consideration or that would require further searching of the prior art on the part of the Examiner. Arguments are also presented below that Applicant believes should render the claims allowable. In the event, however, that the Examiner is not persuaded by the arguments, it is respectfully requested that the Examiner enter the Amendment to clarify issue issues upon appeal.

The specification has been amended to update related application information. Accordingly, no new matter has been entered.

Applicant acknowledges and regrets that some errors and misstatements were inadvertently made in the previous Office Action. The remarks herein are intended to replace the remarks made in the previous office action in their entirety for clarification of the record.

In the Final Office Action, the Examiner rejected claims 1-14 under 35 U.S.C. §102(e) as being unpatentable over U.S. Patent No. 6,898,706 (Venkatesan). Applicants respectfully disagree. Anticipation requires that a prior art reference disclose each and every claim element of the claimed invention. It is respectfully submitted that Venkatesan fails to disclose each in every claim element of the independent claims.

The present invention provides a method and system for delivery of a licensed toolset to a software publisher for creating license-managed software products. The method comprises providing an authorization process, and implementing the authorization process for both a toolset publisher and related toolset and a software publisher and related software product, whereby the same authorization process is used to obtain respective licenses. The authorization process includes creating a first public and private key pair for the software publisher, and creating a second public and private key pair for the software product, wherein at least one of the second private and public keys is digitally signed by the first private key of the software publisher. An authorization program is also created for the software program that has embedded copies of the first and second public keys. The software program and the authorization program are combined, such that when the authorization program is invoked, the authorization program obtains a license for controlling the use of the software program. The license is obtained by creating a license request, encrypting the license request using the second private key, transmitting the license request to a key authority, receiving a license from the key authority with license terms, decrypting the license, and using the license terms to control the use of the software program.

Referring now to the independent claims, in claim 1, Applicants refer broadly to private and public key pairs, while in claim 7 Applicants refer to certificates, which

usually include other information besides keys. According to the preferred embodiment, the software program keys are connected to the software publisher keys so that only that publisher can allow the software program to be authorized. To accomplish this, at least one of the keys of the software program is digitally signed by the private key of the publisher. Using the public key of the publisher, the authorization program can verify that the publisher who signed its product public key is the same publisher who signed the license in response to license request.

In independent claim 7, Applicants refer to signed certificates, which have associated private keys. The public keys are part of the certificate. So in this case, the product certificate is digitally signed by the publisher private key. This allows the authorization program to verify that the publisher who signed its product certificate is the same publisher who signed the license.

In a further embodiment, the publisher of the software program can use a toolset to convert the software program into "a license-managed software product." The publisher uses the toolset and the publisher certificate to create protected software products and to create product certificates for licensing. Thus, the present invention provides a chain of certificates to authorize use of a software program through a license. To run, a software product has to verify the product certificates. Verification means verifying the certificate chain, meaning that the product certificate is cryptographically tied to the proper publisher certificate, which in turn, may be cryptographically tied to a certificate authority certificate. The elegance of the solution is that it allows the certificate authority to control how publishers use the toolset, allows publishers to control how their end-users use their protected software products, and prevents one publisher from authorizing a product from another publisher.

In the previous Office Action, Applicant mistakenly stated that Venkatesan fails to teach or suggest a software licensing mechanism; fails to teach or suggest associating a public and private key pair with a software publisher; fails to teach or suggest generating a license using data extracted from the license request and license terms; and fails to teach or suggest preventing use of the software product on a different computer than that used to generate the license request. Applicant retracts those statements and acknowledges that Venkatesan teaches a software licensing mechanism and the association of a public and private key pair with a software publisher. Venkatesan also teaches that the publisher cryptographically signs the license in response to a license the request.

However, despite these teachings, Venkatesan still fails to address the security of the license request and resulting license, as claimed in the present invention for least the following reasons. First, although Venkatesan may teach creating a first public and private key pair and a second public and private key pair, Venkatesan fails to teach or suggest "combining the authorization program with a software program," as recited in step (a) of claims 1 and 7, where "when the software program is invoked on a computer," the authorization program obtains a license for the software program, as recited in step (a(iv)).

Venkatesan fails to teach or suggest that the authorization program creates a license request. Instead, Venkatesan clearly teaches that "the user" initiates the license request with the publisher through the client PC (e.g., a web browser). Example portions of Venkatesan state:

> After a user has downloaded a watermarked object, then, in order to use that object, the user, through his(her) client PC, electronically transacts, through the Internet, with publisher's web server. In return for

> payment of a specific licensing fee to the publisher, this web server downloads to the client PC an electronic license… (Col. 6, lines 21-27) and (col. 14, lines 35 and 41).
>
> Subsequently, the user, through client PC_j, establishes an Internet session with the publisher's web server and as, indicated by block 540, electronically transacts with that server to obtain a license to use the previously downloaded object.... Once the user makes the selection and authorizes electronic payment for the desired rights, the browser, based on embedded code in the web page, transmits, to the publisher's web server, the rights selection, payment authorization and a computer identification (CID) associated with client PC_j.... Once this information is transmitted to the publisher's web server, that server issues, as indicated by block 550 shown in FIG. 5, an electronic license (L_i) and transmits, as symbolized by line 555, that license to the client PC. (Col. 21, line 66 through col. 22, line 20).

Accordingly, because the license request is manually initiated by the user by interacting with the PC through a Web browser, Venkatesan fails to teach or suggest that the authorization program, which is combined with the software program, creates the license request upon invocation of the software program.

It should be noted that Venkatesan also provides for an enforcer that looks for watermarks in an object whenever the client computer attempts to access a file containing the protected object. It is also believed that the enforcer cannot be considered analogous to the "authorization program" because the enforcer does not generate a license request. In addition, the enforcer is not part of the protected software object. Rather, the enforcer is part of a digital rights management (DRM) system, which in turn is part of the operating system (col. 18. lines 44-45).

Consequently, Venkatesan's fails to teach or suggest a method that combines the authorization program with a software program, where "when the software program is invoked on a computer," the authorization program creates "a license request," as recited in claims 1 and 7.

Second, although Venkatesan may teach the use of a publisher key, Venkatesan also fails to teach or suggest “creating a first private and public key for a software publisher”, as recited in step (a(i)) of claims 1 and 7. The Examiner makes reference to a “secret key”, but Venkatesan describes that this secret key, which is included in the license, “is to decrypt the [software] object. This secret key..., is a symmetric encryption key, i.e., the same key used use by the publisher to encrypt the object (col. 22, lines 25-28). Although Venkatesan’s secret key is used to encrypt the software object, and presumably considered by the Examiner to be “created” for the software program, Venkatesan's secret key is "symmetric", i.e., there is only one. Consequently, there can be no pair of keys for the software program, i.e., a product private key and public key. More importantly, it is believed that Venkatesan's secret key is only used to encrypt and decrypt the software object, but not to digitally sign the second private and public keys for a software program by the first private key of the software publisher, as recited in step (a)(ii) of claims 1 and 7.

One of the elements of the present invention is the fact that the license request created by the authorization program is delivered securely to the key authority. The security is provided by "encrypting the license request using the second public key," as recited in step (a)(iv)(2).

Venkatesan also fails to address providing security for the license request. Venkatesan merely describes that “the user” initiates the license request with the publisher through the client PC (e.g., a web browser), and in return receives a license. Not only is Venkatesan’s license request not encrypted by the second public key for the software program, but the license request appears not to be signed or encrypted all. Consequently, Venkatesan fails to teach or suggest "encrypting the license request

using the second public key," as recited in step (a)(iv)(2).

In the Response to Arguments section of the Final Office Action, the Examiner took issue with Applicant's statement in the previous Amendment that unlike the present invention, in Venkatesan, there is no chaining of certificates. To rebut this argument, the Examiner cited col. 9, lines 25-56 of Venkatesan. However, col. 9, lines 25-56 of Venkatesan make clear that the digital signatures and establishment of chains of trust relate to "components of the O/S and particularly throughout enforcer 600 and DRM system 456," not between software programs, software publishers, and in some embodiments, certificate authorities, as claimed. Accordingly, Venkatesan fails to teach the cooperation of elements in claim 7 that provide for the delivery of secure software license information.

Therefore, it is respectfully submitted that independent claims 1 and 7 are each allowable over Venkatesan for at least these reasons.

In view of the foregoing, it is submitted that claims 1-14 are allowable over the cited references. Because the secondary references stand or fall with the primary references, claims are allowable because they are dependent upon the allowable independent claims. Accordingly, Applicant respectfully requests reconsideration and passage to issue of claims 1-14 as now presented.

Applicants' attorney believes this application in condition for allowance. Should any unresolved issues remain, Examiner is invited to call Applicants' attorney at the telephone number indicated below.

Respectfully submitted,
Strategic Patent Group

April 24, 2006

/Stephen G. Sullivan/
Stephen G. Sullivan
Attorney for Applicant(s)
Reg. No. 38,329
(650) 969-7474